GUIDE TO INSPECTIONS OF

COMPUTERIZED SYSTEMS IN THE

FOOD PROCESSING INDUSTRY

TABLE OF CONTENTS

INTRODUCTION

The> <**use**> <**of**> <**computerized**> <**systems**> <**within**> <**the**> <**food**> <**processing**> <**industry** regulated by the Food and Drug Administration (FDA) continues to increase. The use of computerized system technology is expected to continue to grow in the food industry as the cost of components decrease, as components are continually improved to withstand the rigors of the food processing environment, and as food companies continue to update production facilities, equipment and manufacturing processes in an attempt to produce high quality, high value products. New process design will strive to achieve safe quality products, while at the same time reducing production time and cost. The use of computerized control systems in the production of food products lends itself to fulfilling those goals.

As computer systems become instrumental in providing for the safety of FDA regulated food products, the FDA must verify that proper controls were employed to assure that accurate, consistent and reliable results are obtained from computer control and data storage systems.

This document is intended to serve as a resource for FDA investigators who conduct inspections of regulated food firms that use computers and computer software to control operations and record data that may affect the safety of the finished food product. The Guide was written by the Office of Regulatory Affairs (ORA), Division of Emergency and Investigational Operations (DEIO) and the Center for Food Safety and Applied Nutrition (CFSAN). If you discover errors in printing or have suggestions for changes which you feel will contribute to the goal of increasing inspectional quality and uniformity, please communicate your written comments or suggestions to DEIO, HFC-130 or send via e-mail (internal Banyan address) to: DEIOFOODS@LISTS.LOCAL@FDAORAHQ.

CHAPTER 1: REGULATION OF COMPUTERIZED SYSTEMS

A. FOOD, DRUG AND COSMETIC ACT

FDA's authority to regulate the use of computers in food plants is derived from the Food Drug and Cosmetic (FD&C) Act Section 402 (a) (3) "A food shall be deemed to be adulterated if it consists in whole or in part of any filthy, putrid, or decomposed substance, or if it is otherwise unfit for food,"Section 402 (a) (4)"A food shall be deemed to be adulterated if it has been prepared, packed or held under insanitary conditions whereby it may have become contaminated with filth, or whereby it may have been rendered injurious to health," Section 412, Requirements for Infant Formula, and the Emergency Permit Control section 404 for thermally processed low-acid canned and acidified low-acid foods.

Documents governing the use of computerized systems under the PMO (Pasteurized Milk Ordinance) Cooperative Program contain additional requirements and/or guidelines.

B. GOOD MANUFACTURING PRACTICE REGULATIONS (CFR TITLE 21)

The following information provides a guide to those areas of specific 21 CFR regulations that have been or may be used to regulate the use of computerized systems in food manufacturing plants. This guide may not include all CFR references under which computerized systems can be regulated.

PART 11 ELECTRONIC RECORDS AND SIGNATURES

This regulation allows regulated industry to electronically maintain those records required to be kept by the current regulations. Records which are electronically maintained following the provisions of 21 CFR Part 11 will be recognized as equivalent to traditional records. In addition electronic signatures used as per the provisions of this regulation will be equivalent to full handwritten signatures and initials, unless specifically exempted by regulations issuing after the effective date of the regulations. In order to do so a firm must certify to the agency that validated controls are in place.

PART 106 INFANT FORMULA QUALITY CONTROL PROCEDURES

On July 9, 1996 the FDA published in the Federal Register proposed amendments to CFR Title 21 parts 106 and 107 titled Current Good Manufacturing Practice, Quality Control Procedures, Quality Factors, Notification Requirements, and Records and Reports, for the Production of Infant Formula which add specific requirements for the use of computerized equipment in the manufacturing of infant formula. The proposed requirements include:

1. Definitions of hardware, software, system, and validation.
2. Requirements that systems be designed, installed, tested and maintained in a manner that will insure that they are capable of performing their intended functions.
3. Requirements for system validation and calibration.
4. Requirements for verification of input/output data to insure its accuracy.
5. Requirements for revalidation when system changes are made.
6. Requirements for making and retaining records concerning electronic systems.

(Note the proposed regulations have been published but are not yet final)

PART 110 CURRENT GOOD MANUFACTURING PRACTICE IN MANUFACTURING, PACKING

AND HOLDING HUMAN FOOD.

FDA regulations **21 CFR Part 110**, promulgated under the authority of the FD&C Act, do not specifically address the use of computerized systems. However, there are many inferences to the agency's authority over such systems.

1.) **Subpart C Equipment, 110.40 (a)** requires That "The design, construction, and use of equipment and utensils shall preclude the adulteration of food with lubricants, fuel, metal fragments, contaminated water, or any other contaminants."

2.) **Subpart C Equipment, 110.40 (f)** requires that "Instruments and controls used for measuring, regulating, or recording temperatures, pH, acidity, water activity, or other conditions that control or prevent the growth of undesirable microorganisms in food shall be accurate and adequately maintained."

3.) **Subpart E, Production and Process Controls, 110.80** states that "all reasonable precautions shall be taken to ensure that production procedures do not contribute contamination from any source." It continues in **110.80 (b) (2)** that "all food manufacturing . . . shall be conducted under such conditions and controls as are necessary to minimize the potential for growth of microorganisms, or for the contamination of food."

Implied and explicit references for the need to have computerized controls be accurate and reliable may be found in other locations of the GMPs Part 110 depending upon the function of the computerized system in the food process.

PART 113/114 THERMALLY PROCESSED AND ACIDIFIED LOW-ACID CANNED FOODS.

FDA's Center for Food Safety and Applied Nutrition (CFSAN) has determined that the use of computerized systems to record LACF processing information and/or to perform real-time process deviation corrections as required under **21 CFR Part 113, Thermally Processed Low Acid Canned Foods in Hermetically Sealed Containers**, is acceptable. CFSAN reviews these systems to determine the computerized system performs the function in a manner that is equivalent to the intent of the regulations.

Computer equipment vendors who wish to market their computer systems for LACF record keeping functions and/or to perform real time process deviation corrections, have been advised they may submit their computer systems to FDA's CFSAN for a review which may consist of:

1. a visit to FDA by the system vendor or user to explain the operation of the computer system;
2. a visit by FDA to the vendor to examine the hardware and software development, validation and documentation procedures; and,
3. a visit by FDA to a production site to evaluate the computerized record keeping/control system under commercial conditions.

In the past, vendors who submitted their computerized systems to this type of review and were found to be satisfactory, received a letter stating that FDA found the computerized system, as evaluated, to meet the intent of the regulations. Use of this voluntary submission of computerized systems to FDA for evaluation subjected the vendor to requirements to update FDA when substantial changes are made in the computerized system, a requirement that FDA investigators would be provided on-site access to the vendor's computer equipment/software operating instructions, and a requirement that the vendor instruct the customer in procedures for using, maintaining and updating the computer software and equipment.

Field Investigators should be aware that LACF computer controlled recording and real time process deviation correction systems do exist that have been evaluated by FDA. If the firm claims that the computerized system and/or software has been evaluated by FDA the firm should have on hand a copy of the FDA letter to the vendor stating that the computerized system or software has been evaluated and found to meet the intent of the regulations for record keeping. If there are questions or concerns, CFSAN (Chief Regulatory Food Processing and Technology Branch, HFS-617, Tel: 202-205-4842) should be contacted to verify that the vendor has been issued a letter or handled otherwise.

There is no requirement that computerized systems used to control or record LACF functions be evaluated by FDA prior to use. When computerized control/record keeping systems are encountered that have not received prior review by CFSAN, the Field Investigator must make a complete evaluation of the computerized system (See Inspection Concepts for Computerized Systems). A copy of the report should be submitted to HFS-617 for evaluation.

Computerized systems are used not only for the generation of LACF processing records, but for control functions such as: formulation control, process deviation calculations, process temperature, process pressure, process timing and container closure examination. The control of functions that may be critical to ensuring a safe food product, must also be reviewed by the investigator to determine that they meet the intent of the LACF regulations.

PART 123 FISH AND FISHERY PRODUCTS.

FDA's HACCP regulations Title 21 CFR Part 123-Fish and Fishery Products does not specifically state requirements for the use of computers and computer software except for section 123.9 (f) which requires that appropriate controls are implemented to ensure the integrity of electronic data and signatures. It is implied elsewhere in the regulations that systems used to control the production of Fish and Fishery Products shall not cause the products to be adulterated. Computerized systems controlling critical control points should be evaluated using HACCP techniques by the manufacturing firm during development of the firm's HACCP Plan.

PART 129 BOTTLED DRINKING WATER.

Title 21 CFR Part 129- Processing and Bottling of Bottled Drinking Water, Sub-part C-Equipment section **129.40** requires that all equipment used in the bottling operation be suitable for use. **Section 129.80 of Sub-part E production and Process Controls** requires that the treatment of product water shall be performed by equipment which does not adulterate the finished product.

C. INSPECTION CONCEPTS FOR COMPUTERIZED SYSTEMS

The investigator must keep in mind the limitations of specific regulations regarding the use of computers in food processing plants, other than infant formula manufacturers, and FDA's lack of specific authority to examine computer software and computer hardware documentation in those plants. However; as long as the computerized system controls or records part of or the entirety of a manufacturing process, the manufacturer is responsible for establishing that the computerized system functions as it was intended to function. During the inspection of a food manufacturer where a computerized system is in use, the investigator is entitled to be provided with the assurance that the process functions controlled by the computer operate as designed. It is important to remember that computer control and/or record keeping systems must provide for accurate, reliable and consistent results.

The investigator should evaluate the operations of computerized systems during the inspection to determine if the use of the computer and/or software may lead to adulteration of the finished food product. Many computers used in the food industry may be used for quality purposes only and will not affect the safety of the food product. For example, if the computer is controlling an oil fryer temperature in a potato chip factory, the criticality of the temperature control function may be a matter of resulting in a batch of darker tinted chips. On the other hand, if the computer system controls the sterilization temperature of an LACF process, it is critical that the computerized function provide consistent and reliable performance. HACCP (Hazard Analysis Critical Control Point) inspection concepts can be used to identify those critical food processing and documentation steps controlled by a computerized system.

When a computerized system is encountered in a food establishment, it may be useful for inspection purposes to begin with a broad overview of the system(s). Determine exactly which functions are under computer control, monitoring or documentation and which are not. For each function of a food process under computer control determine the general system loop (sensors, central processor, activators). For example, the general system loop for a steam retort under computer control could consist of temperature/pressure sensors connected to a microprocessor that transmits commands to steam/pressure control valves. The overview should enable the investigator to identify those computer controlled functions that are critical to food product safety. **These are the functions of the computerized systems that merit closer inspection**.

Often food manufacturing firms may not have on hand detailed information covering the development and validation of the software and microprocessors used in their processing systems. Many firms buy the microprocessors as off the shelf technology from the equipment vendor. The investigator should then determine the functions of the control system in as much detail as possible. If the firm has a schematic drawing of the computerized system this may be obtained or the

investigator may prepare a simplified schematic drawing, which will be helpful in explaining the computerized systems operations and configuration. The drawing should include major input devices, output devices, signal converters, central processing unit(s), distribution systems, and how they are linked. During the inspection identify the manufacturers and suppliers of important computer hardware, including the make and model designations where possible. Hardware to identify this way includes CPUs, disk/ tape devices, CRTs, printers, input sensors, output activators and signal converters. Proper identification of hardware will enable further follow-up should that be needed. If the firm does not have detailed information on the computerized control system, the investigator should obtain any limited information that is available.

During the inspection identify key computer software used by the firm. Of particular importance are those software routines that control and document critical production steps and laboratory testing to support critical functions (such as the addition of nutrients to infant formulas). A schematic of the major software routines and how they interact should be obtained from the firm or prepared by the investigator based on observation or other documentation. Directories or list of software routines and subroutines can sometimes be displayed on the CRT display or printed out. For some application software a list of routines can only be provided by the software vendor and may not be available at the manufacturing firm.

Determine how software is set up to handle input data. For example, determine what equations are used as the basis for calculations in a routine. When a food manufacturing process is under computer control describe, in simplified form such as a flow chart, how input is handled to accomplish the various steps in the process. This does not mean that a copy of the computer software source code itself needs to be reviewed. However, before applying computerized control and record keeping to a food process there usually needs to be some document, written in English, setting forth in logical steps what needs to be done; it would be useful to review such a document in evaluating the adequacy of conversion from manual to computerized processing.

Observation of the system as it operates can be used to determine if critical factors such as revolutions per minute (rpm), vent times, temperatures, pressures, thermal process times, and documentation are being controlled by the computerized system. Operation of the system should be observed through several process cycles. However, end product testing (observation) of the computer system should not in itself be relied upon to provide assurance that the system is operating as designed. End product observation will not test all of the different possibilities that a computer system will respond to during a process. Importantly it will not reveal the systems behavior at the permissible limit of functionality and performance. The only way to develop confidence that the computer system is going to function correctly is to have a validation program as part of the design, coding, testing, and implementation steps **(See Section on Computerized System Validation).**

The investigator should determine who is responsible for programming the system, how the system is programmed, the name and number of programmable functions, if the programming functions are password or otherwise protected, and who is responsible for record review (including system and process documentation records) and computerized system verification.

It is also important to find out if the operator or management can override any of the computer control functions. If operator/management override of computer functions are possible details on how this is done, what overrides are possible, and how overrides appear in the processing record should be determined.

The investigator should find out how the system handles deviations from set or expected results during processing. If the computer system can adjust critical manufacturing parameters, calculate new manufacturing parameters or choose alternate preprogrammed procedures the investigator must determine the parameters for computing or selecting the alternate procedures.

During inspections of food firms using computerized systems to control and/or record critical functions (e.g., retort sterilization temperature, smoked fish internal temperatures) or to control other factors critical to the food manufacturing process (e.g., viscosity of a thermally processed LACF, water activity of a dehydrated food) the minimum information to obtain would include:

a. The equipment specifications for software and hardware.
b. The critical factors controlled by the system.
c. How the critical factors are controlled?
d. How does the firm ensure that the microprocessor or computer is indicating the correct information (validation)?
e. How and how often is the equipment calibrated and/or checked for accuracy?

Documentation showing that a computerized operation may contribute or contributes to the adulteration of a food product will take an extended effort by the investigator. Development of evidence of food adulteration caused by the operations of a computerized system should be discussed with CFSAN/OFP/Division of Enforcement (HFS-605).

During the inspection of food processing facilities the responsibility of the food manufacturing firm regarding their use of computerized systems to control or record the critical safety aspects of food manufacturing should be discussed with the facilities management. The FDA investigator should make the firm's management aware that a computerized system includes the hardware, software, personnel, and operating procedures required to operate the system. Management at the firm should be made aware that the computerized system should be validated in place under actual operating conditions by the firm **(See Section on Computerized System Validation).**

The applicable sections of the listed references should be used, in addition to this guide when inspecting firms using complex computerized systems.

CHAPTER 2 COMPUTER SYSTEM TECHNOLOGY

A. TECHNOLOGY OVERVIEW

In recent years digital electronic controllers have replaced the relays and sensing switches of mechanical/analog-electrical control systems used in food processing. Digital control systems may range from the single-loop controller to complex high-end computer systems.

If the function to be controlled consists of numerous sequential (logical) steps, the controlling device can be a first-level computer device called a logic controller. The logic controller may be set up as a single loop controller.

A single loop controller would be responsible for controlling one function, such as temperature in a steam kettle. The controller loop would be programmed to control the kettle temperature within set temperature parameters. The loop would consist of the microprocessor controller, a temperature sensor, an actuator for the steam valve and a digital/analog signal converter.

Simple single loop controllers contain Read Only Memory (ROM) which is manufactured into the controller or programmed into the controller by using Programmable Read Only Memory (PROM), Erasable Programmable Read Only Memory (EPROM) or Electronically Erasable Programmable Read Only Memory (EEPROM).

PROM is field programmable by the manufacturer or customer once only by burning out fuses in the PROM microprocessor chips. EPROM is electronically programmed by the manufacturer or user. EPROM microprocessor chips are reprogrammed by exposing the chip to an ultraviolet light source that resets the original chip configuration. EEPROM microprocessor chips can be reprogrammed by electronically erasing the memory on the chip. ROM is normally used to control functions where the options of the customer or operator do not need to be changed. Random Access Memory (RAM) using battery backed volatile memory components is another type of memory component. This memory requires a power supply but lends itself to modification and

reprogramming. Advanced microprocessor or computer systems would normally use a combination of ROM and RAM to program control of processing functions.

A more advanced system would use a programmable logic controller (PLC) which would allow the operator or firm to alter the control limits of the controller **(See Appendix 2).** This type of controller would use algorithms (a programmed procedure for solving a problem) to control the loop. Algorithms are written to provide the microprocessor with a logical sequence of events for solving a problem **(See Appendix 3).**

Control of multiple parameters such as temperature, pressure, pumping rate, rotation, etc. may be performed by installation of several loop controllers controlled by one PLC, microprocessor or computer.

Computers are different from hardwired controls in three major categories. To provide for adequate control of critical control points in food processing and/or documentation, the design of the computerized controls must address these three major areas:

1. First, unlike conventional hardwired systems, which provide for full-time monitoring of critical functions, the computer performs its task sequentially, and the computer may be in real time contact with the sensor for only one millisecond. During the next 100 milliseconds (or however long it takes the computer to cycle one time through its task), the critical sensor is not monitored. Normally this is not a problem, because most computers can cycle through their program steps many times during one second. The problem occurs when the processing computer is directed away from its task by another computer, or the computer software program is changed, or a seldom used JUMP, BRANCH or GO TO Instruction diverts the processing control computer away from its control or monitoring function.
2. In a computerized system the control logic may be easily changed if the computer software can be easily changed. Some security measures are needed to ensure that the computer has the correct software in place.
3. Some computer experts have stated categorically that no computer software can be written error-free. While this may be true for very large software routines with thousands of lines of code, most of the software routines used for control and documentation of critical functions in food processing are relatively brief. Software that controls functions critical to food safety

can and should be made error-free.

B. COMPUTERIZED SYSTEM HARDWARE

Input Devices: Equipment that translates external information into electrical pulses that the computer can understand. Examples are thermocouples, RTDs (Resistance Temperature Devices) flow meters, load cells, Ph meters, pressure gauges, control panels, modems, cathode ray tubes (CRT), data entry touch screens and operator keyboards.

Examples of functions are:

a. Thermocouple/RTD provides temperature input for operation of a retort.
b. Flow meter provides volume of liquid component going into a mixing tank.
c. Operator keyboard used to enter weights, batch, menu number and other processing information.

Output Devices: Equipment that receives electrical pulses from the computer and either causes an action to occur, generally in controlling the manufacturing process functions, or passively records data. Examples are valves, switches, motors, solenoids, cathode ray tubes (CRTs), printers, and alarms. Examples of functions are:

a. Solenoid activates the impeller of a mixer.
b. Valve controls the amount of steam delivered to a thermal process.
c. Printer records significant events during a sterilization process.
d. Alarm (buzzer, bell, light, etc.) sounds when temperature in a holding tank drops below the desired temperature.

Most output devices will be in proximity to the food processing equipment under control, but not necessarily close to the CPU. Some output devices such as printers may be located away from the immediate processing area.

Signal Converters: Many input and output devices operate by issuing/receiving electrical signals that are in analog form. These analog signals must be converted to digital signals for use by the computer; conversely, digital signals from the computer must be converted into analog signals for use by analog devices. To accomplish this, signal converter devices are used.

Most signals are analog until they reach the computer. Transducers are often used to send the analog signals to the computer or PLC. For example a temperature measuring device will be attached to a transducer within a very short distance from the device itself. The transducer will have a defined span (0-150 C) to send its 4-20 milliamp signal to the computer, where it is then converted into a digital value. Digital transducers are available, but their expense has resulted in limited use. Many PLC systems will have only 8 bit A/D converters, which means that the span on the 4-20 milliamp transducer is now critical to the resolution of the signal as seen by the computer and thus, its ability to control the function. Another problem with transducers is that some new ones are "auto-calibrating." What this means is that when the system is powered up the base line and span of the transducer is recalibrated or adjusted, and this results in an adjustment in the signal sent to the computer that may be different from the device's original calibration. For example, temperature values may change as much as 0.5 C from day-to-day because of this. A properly validated system will have taken this into account, which means that maintenance of the system and the proper replacement of sensors and transducers is critical to the systems ability to control the food manufacturing process functions as originally designed. Design specifications should be reviewed to determine the type and model number of all the sensors and transducers to insure that as maintenance was performed on the system the correct electrical components were used.

Normally the only part of a control system that Communicates using a digital signal is the computer process control network. Most all A/D signal conversion occurs immediately at the PLC or computer and all PLC-PLC, PLC-computer and computer-computer interaction is digital.

Proper input/output signal conversion is important if the computer system is to function accurately. Poor signal conversion can cause interface problems. For example, an input sensor may be feeding an accurate reading to a signal converter, but a faulty signal converter may be sending the CPU an inappropriate signal. In some cases faulty signal converters may be recognized by observing the difference between what is indicated on a separate readout or by a separate instrument and the reading presented by the computerized system. For example if an RTD readout indicated a temperature of 80 C in a steam jacketed kettle and

the computerized system CRT reads 100 C you might suspect a faulty signal converter. One way to make sure that proper signal conversion is going on is to make sure that the original specifications for the system agree with the maintenance records for the system. If the maintenance records are not available the original specifications of the system should be checked against the equipment on the system. Proper signal conversion is best addressed by performing input/output checks. The food manufacturer needs to have in place a procedure by which all input/output signals are checked for accuracy. **(See Monitoring of Computerized Operations, Input/ Output Checks)**

Central Processing Unit (CPU) This is the controller containing the logic circuitry of a computer system that conducts electronic switching. The size of the computer needed for control depends upon the number of loops to be controlled and whether the system is set up as an independent, centralized, or a distributed system. Logic circuits consist of three basic sections - memory, arithmetic, and control. The CPU receives electrical pulses from input devices and can send electrical pulses to output devices. It operates from input or memory instructions. Examples and functions are:

a. Programmable controllers used for relays, timers and counters.
b. Microprocessors used for controlling a steam valve, maintaining pH, etc. They consist of a single integrated circuit on a chip. This is the logic circuit of a microcomputer and microprocessors are often the same as a microcomputer.
c. Microcomputers and minicomputers used to control a sterilization cycle, keep records, run test programs, perform lab data analysis, etc.
d. Mainframe computers are generally used to coordinate an entire plant, such as environment, production, records, and inventory.

Distribution System: The method used for interconnection of two or more computers.

In the independent system, each manufacturing operation is controlled by its own PLC or microprocessor. If a control system fails, the remainder of the systems would continue to operate.

In a centralized system, all data would be collected and analyzed by a central computer. This provides for quick capture of all processing information and for control from a central location. Failure of this control system would mean that all processing systems would be down.

In the distributed system, a PLC or microprocessor can be used for independent control of each production system. The process microprocessor is then used to supply information to a separate host computer that captures all processing control data for storage and printing. The host computer in turn stores process software and is used to program the logic controls of the microprocessor(s).

In distributed systems it is important to know how errors and command overrides at the computer are related to operations at another computer in the system. For example, if each of three interconnected microcomputers runs one of three retorts, can a command entered at one unit inadvertently alter the sterilization cycle of a retort under the control of a different microcomputer on the line? Can output data from one be incorrectly processed by another unit? The limits on information and command flow within a distributed system should be clearly established by the firm.

Networks are generally extensions of distributed processing. They may consist of connections between complete computer systems that are geographically distant or they may consist of computer systems on a local area network (LAN) in the same facility.

If the firm is on a computer network it is important to know:

a. What output, such as batch production records, is sent to other parts of the network;
b. what kinds of input (instructions, software programs) are received;
c. the identity and location of establishments that interact with the firm;
d. the extent and nature of monitoring and controlling activities exercised by remote on-net establishments; and,
e. what security measures are used to prevent unauthorized entry into the network and possible unwarranted food process alteration, or obliteration of food process controls and records.

Peripheral Devices: All computer associated devices external to the CPU can be considered peripheral devices. This includes the previously discussed input and output devices. Many peripheral devices can be both input and output, they are commonly known as I/O devices. These include CRTs, printers, keyboards, disk, modems and tape drives.

C. ENVIRONMENTAL/EMI HAZARDS

Location: Potential problems have been identified with location of CPUs signal transmission lines and peripheral devices. These Include:

Hostile Environments: Environmental extremes of temperature, humidity, static, dust, power feed line voltage fluctuations, and electromagnetic interference should be avoided. Such conditions may be common in certain operations and the investigator should be alert to locating sensitive hardware in such areas. Environmental safeguards may be necessary to ensure proper operation.

Electromagnetic Interference (EMI): Low voltage electrical lines from input devices to the CPU are vulnerable to electromagnetic interference. EMI may result in inaccurate or distorted input data to the computer. Therefore, peripheral devices should be made immune to electromagnetic interference (EMI) such as electrical power lines, motors, portable telephones, walkie-talkies, radio/TV broadcasts, and fluorescent lighting fixtures. Peripheral devices and signal transmission lines should be located as far as possible from sources of electromagnetic interference. Shielding of signal transmission lines, grounding, filters, circuit design and proper design of the device's cabinet or housing are acceptable methods to prevent EMI.

Distance Between CPU and Peripheral Devices: Device proximity to the PLC/computer may be important concerning loss of signal due to electrical resistance of the signal transmission lines. To correct this problem the device may be located near the PLC/computer or signal transmission lines having less electrical resistance (i.e. 2 wire vs. 4 wire RTD) may be used.

Proximity of Input Devices to Food Processing.

Input devices such as employee interfaces should be located as close as possible to the operation being controlled.

D. MAINTENANCE/CALIBRATION

Computer systems normally require a minimum of complex maintenance. Electronic circuit boards, for example, are usually easily replaced and cleaning may be limited to dust removal. Diagnostic software is usually available from the vendor to check computer performance and isolate defective integrated circuits. Maintenance procedures should be included in the firm's standard operating procedures. The availability of spare parts and access to qualified service personnel are important to the operation of the maintenance program.

The firm should use replacement parts which meet the specifications of the original computer system design or the system should be revalidated to document that the replacement parts perform as per the original specifications of the computer system.

Sensors used as part of the computerized system, monitoring or controlling process functions, should be checked for accuracy in the set operating range of the function being controlled or monitored during production. For example if an RTD is used to sense the temperature of a retort system operating at 250 F, the RTD should be accurate at 250 F and not just at some lower temperature, such as at 212 F.

Computerized systems used to control, monitor or record functions that may be critical to the safety of a food product should be checked for accuracy at intervals of sufficient frequency to provide assurance that the system is under control. If part of a computerized system that controls a function critical to the safety of the food product is found not to be accurate, then the safety of the food product back to the last known date that the equipment was accurate must be determined. (e.g., an RTD is providing a signal which indicates that a thermal process is operating at 95øC, when is fact the process is operating at 90øC. If 90øC is below the firms established critical limit for food safety, the safety of the food may be in question. If this was noted on March 23 and the RTD was last checked for accuracy on January 1, the food processed from January 1 to March 23 should be evaluated for safety).

The manufacturers/vendors of computerized system components normally recommend minimum maintenance schedules including accuracy checks of their components.

E. COMPUTERIZED SYSTEM SOFTWARE

Software is the term used to describe the total set of programs, procedures, rules, and any associated documentation pertaining to the operation of a computerized system and includes: application, operating system, and utility software used by the computerized system **(see Glossary of Computerized System and Software Development Terminology, August 1995).**

Name: Software routines are usually named with some relationship to what they do, i.e., Production Initiation, Batch Production or Alarm. The name of the software may be followed by a version number (i.e., DOS 6.0) that indicates where that particular software version falls in the release history of the software (i.e., between DOS 5.2 and DOS 6.2)

Function: Software routines should have a defined function or purpose, i.e., start production, record and print alarms, or calculate Fo.

Input: Inputs, such as thermocouple signals, timer, or analytical test results should be identified.

Output: Output signals generated by the software may result in a form of mechanical action (valve actuation) or recorded data (generation of records). Outputs should be identified.

Fixed Set point: This is the desired value of a software function variable that cannot be changed by the operator during execution. Determine major fixed set-points, such as desired time/temperature curve, desired pH, etc. Time may also be used as a set point to stop the computer controlled process to allow the operator to interact with the system.

Variable Set point: This is the desired value of a software function variable that may change from run to run and must usually be entered by the operator. For example, entering the initial temperature of a LACF thermal process for each retort load.

Fuzzy Logic: Computerized systems utilizing fuzzy logic are increasingly being developed and used in food processing. Fuzzy logic differs from conventional logic in that the information used to control the system is neither definitely true nor false. Fuzzy logic control is carried out by implementing linguistic decision rules that come from the experience of operators or the knowledge of industry experts. Input from several sources may be used by the fuzzy logic controller to form the output decision of the computer system. A complete discussion of fuzzy logic control systems is beyond the scope of this document, the investigator should however be aware that this type of logic controller may be found in food manufacturing. Examples of everyday equipment using fuzzy logic would be: Television sets with automatic color control, hand held camcorders that compensate for operator movement and anti-lock braking systems used on automobiles. Potential problems with these type of control systems is that they can be programmed where there is no fixed set point by which the software function is controlled. When fuzzy logic controllers are used to control factors critical to the safety of a food manufacturing process a more detailed review of the control system is warranted. Determine if a record is made of control of the critical factor by the computerized system. A permanent record or an alarm function may be used to verify that a fuzzy logic controller controls each critical factor at or beyond its critical limit.

Edits: Software may be written to reject or alter certain input or output information that does not conform to some predetermined criterion or otherwise fall within certain pre-established limits. This is an edit and it can be a useful way of reducing errors; for example, if a certain piece of input data must consist of a four-character number, software edits can be used to reject erroneous entry of a five-character number or four characters comprised of both numbers and letters. On the other hand, edits can also be used to falsify information and give the erroneous impression that a function is under control. For example, a software output edit may add a spurious "correction" factor to temperature values that fall outside the Pre-established limits, thus turning an unacceptable value into an "acceptable" value. It is, therefore, important to attempt to identify significant software edits during the inspection, whenever possible. Sometimes such edits can manifest themselves in unusually consistent input/output information.

Software Over-rides: Software may be designed so that the sequence of programmed events or edits can be overridden by the operator. For example, a function controlling routine may cause an ingredient auger motor to stop when the weigh scale contents reach a predetermined weight. The software may prevent the auger motor from resuming activity until the weight has dropped back to the established set point. However, the same software may allow an operator to override the stop and reactivate the auger motor even at a weight that exceeds the set point limit. It is therefore important to know what overrides are allowed, if they conflict with the firm's operating instructions and how the system documents the override event(s).

Software Development: During the inspection determine if the computer software used by the firm has been purchased as "off the shelf" from outside vendors, developed within the firm, prepared on a customized basis by a software producer, developed by a third party vendor or some combination of these sources. Some software is highly specialized and may be licensed to food establishments. If the software used by the firm is purchased or developed by outside vendors, determine which firms prepared the software.

Sometimes "off the shelf" or customized software may contain segments (such as complex algorithms) which are proprietary to their authors and which cannot normally be readily retrieved in program code without executing complex code breaking schemes. In these cases the buyer should obtain validation documentation from the supplier to ensure that the software will perform as designed. If the food manufacturer is using such software to control or monitor a critical control point in the food process, determine what steps the firm has taken to verify that the software is performing as it was designed. Where food firms develop their own application software, review the firm's documentation of the approval process. This approval process should be addressed in the firm's written development instructions. It may be useful to review the firm's development (English) documents that formed the basis of the computer software **(See Software Development Activities, July 1987, U.S. Department of Health and Human Services, Food and Drug Administration).**

Software Security: Determine how the firm prevents unauthorized software changes and how data is secure from alteration, inadvertent erasures, or loss. Determine whom in the firm has the ability and/or is authorized to write, alter or have access to software. The firm's security procedures should be in writing. Security should also extend to devices used to store software, such as tapes and disks. Determine if accountability is maintained for these devices and if access to them is limited.

An important part of software security is change control. The firm should have in place a written procedure by which changes are made to software. This will include identification of a software error, how it was corrected, who performed the correction, did the changes influence any other portions of the software program, were the changes validated specifically and then as they related to other portions of the software program, and how the changes were documented. Software has a circular life-cycle that requires a defined maintenance procedure be followed **(See Computerized System Validation).**

F. PERSONNEL QUALIFICATIONS

Personnel operating, maintaining and programming computerized control systems should have adequate training and experience for performance of their assigned duties. Determine the extent of operator, system managers, and computer system technical personnel training in the functions, requirements and operation of the computerized system. Training should include not only system operation but cover the significance of system faults (bugs), regulatory requirements, system changes, security procedures, manual operation of the system, and documentation of system errors. Training of computerized system personnel should be documented by the manufacturing firm.

The investigator should determine the key computerized system personnel during the inspection. This may include not only the firm's own employees but outside vendors or consultants. For each of the key employees, determine to the extent possible, that employee's responsibility for the computerized system. It is important that technical personnel are available or can be reached during computerized system failures.

G. PROCESS DOCUMENTATION

Most computerized systems are capable of generating accurate and detailed documentation of the food process under computer control. What is important is that the computer generated records contain all of the information required by the CGMPS. For example, if production records are generated by computer, determine if they contain all of the information required to be in each record (s).

The firm should have security measures in place to insure that data captured by the computerized system cannot be altered. If provisions are made to allow correction of data entries, the entry should identify the person making the changes and the reason for the change should be identified. For example an operator misreads a temperature indicator and enters the information into the system. The computer system then alarms the operator that the entry is out of the correct range. The operator then enters the correct temperature which is accepted by the system. All of the above should be captured on the firms records. For those firms storing records electronically, provisions should be made to store the records in a format which cannot be easily altered.

Computerized systems generating critical control monitoring records must be capable of recording the lowest and/or highest value (depending upon the critical control limits) measured between two recording points. (for example, the sensor sends a vessel pressure to a computer continuously, even though the signal is recognized by the computer every few milliseconds, it is only printed out once every 2 minutes, it may be critical to know the lowest vessel pressure during that 2 minute period).

Electronic records must be maintained in a format that can be presented to the investigator in a readable form. This could be in the form of electronic data that can easily be accessed and read by common computer software or in the form of accurate hard copy documents produced from electronic records maintained by the firm.

Electronic Signatures if used should be controlled by the firm under written operating procedures, which insure that the electronic signature is a valid representation of the individual making the entry. Operator entry codes should be protected so that they can be used only by the person assigned that code. Electronic signatures should meet all of the requirements of FDA's final rule, 21 CFR Part 11, regarding electronic signatures.

CHAPTER 3 COMPUTERIZED SYSTEM VALIDATION

A computerized system includes: the computer hardware, computer software, peripheral devices, personnel, and computer system documentation (including computer hardware and software manuals, specifications for peripheral devices and standard operating procedures).

The computerized system used to control critical functions in food processing should be validated in its entirety.

The suitability of a computerized system for the tasks assigned to food production should be shown through appropriate tests and challenges. The depth and scope of computerized system validation will depend upon the complexity of the system and its potential effect on food safety. The validation program need not be elaborate but should be sufficient to support a high degree of confidence that the computerized system (software, hardware, personnel and operating procedures) will consistently perform as it is supposed to **(See System Testing Reference "Software Development Activities Report)**. Although various components of the computerized system may be tested separately (qualification), the total computerized system should be validated. Validation requires the system, as it will be configured and used in production to be shown to behave as expected (defined or specified) not only for normal conditions and inputs, but importantly that it continues to provide control and useful, meaningful outputs when unusual, or unexpected conditions and events occur and when inputs occur at the specified ranges or boundaries. That is, worst case conditions must be identified and tested. It is vital that a firm have assurance that software routines, especially those that control critical manufacturing functions, consistently perform as they are supposed to within pre-established operational limits. Determine who conducted the computerized system validation and how key computerized system routines were tested.

In considering computerized system validation, the following points should be addressed:

1. Does the capacity of the hardware match its assigned function? For example, in a system using an RTD for temperature control, is the RTD capable of sensing temperatures through out the processing control range, has the RTD been checked for accuracy in the operating temperature range(s), does the computer receive an accurate signal from the RTD, and does the computer react to the RTD signals as designed?
2. Have operational limits been identified and considered in establishing production procedures? For example, a PLC may be able to only receive input from two thermocouples at one time. This would limit the number of locations at which temperatures could be obtained in this manufacturing process.
3. Does the software match the assigned operational function? For example, if software is assigned to generate complete thermal processing records for a LACF process, then it should account for all of the information required to be recorded for that retort system as required by the GMPs Part 113.
4. Have test conditions simulated "worst case" production conditions? A computerized system may function well under minimal production stress (as in a vendor's controlled environment) but falter under high stresses of equipment speed, data input overload or frequent or continuous multi-shift use, unexpected sequences or order of events and a harsh environment. Therefore, it is insufficient to test the computerized system for proper operation during a short interval, when the system will be called upon in worst case conditions to run continuously for days at a time. Some firms may test the circuits of a computer by "feeding" it electrical signals from a signal simulator. The simulator sends out voltages designed to correspond to voltages normally transmitted by input devices. When simulators are connected to the computer, the software program should be executed as if the emulated input devices were actually connected. These signal simulators can be useful tools for equipment qualification; however, they may not pose worse case conditions and their accuracy in mimicking input device performance should be established. In addition, validation runs should be accomplished on line using actual input devices.
5. Have computerized system tests been repeated enough times to assure a reasonable measure of consistent reproducible results? In general, at least three consecutive, successful test runs should be made to cover different operating conditions. If test results are widely divergent they may indicate a software bug or an out of control state.
6. Has the validation program been thoroughly documented? Documentation should include a validation protocol and test results that are specific and meaningful in relation to the attribute being tested. For example, if a temperature sensor's reliability is being tested, it would be insufficient to express the results merely as "acceptable," without other qualifying data such as temperatures observed, duration of the test, and the temperature range tested. The individual(s) responsible for conducting, reviewing and approval of the system validation should be identified in the documentation.
7. Are documented systems in place to initiate revalidation when significant

changes are made to the computerized system or when computer system errors are noted? Documentation should include the reason for the system change, the date of the system change, the changes made to the computerized system, and identification of who made the changes. Revalidation is indicated, for example, when a major piece of equipment such as a circuit board or an entire CPU is replaced and when software changes such as time, temperature, sequence of routine events, data edits or data handling are made. Sometimes identical hardware replacements may adequately be tested by using diagnostic programs available from the vendor. In other cases, such as when different models of hardware are introduced, more extensive testing under worst case production conditions, is indicated.

Computerized system vendors routinely perform an installation qualification to ascertain that the equipment is functioning within the hardware manufacturers specifications after being installed. However, hardware qualification is only part of the verification process and the complete computerized system should be validated.

The ultimate responsibility for suitability of the computerized system used in food processing rests with the food manufacturer. Computerized system validation data and protocols should be kept at the food manufacturer's facility. When validation information is produced by an outside firm, such as the computer vendor or software developer, the records maintained by the food establishment need not be all inclusive of voluminous test data; however, such records should be reasonably complete (including system specifications, protocols and general results) to allow the food manufacturer to assess the adequacy of the system validation. A mere certification of suitability from the vendor, for example, may be inadequate.

CHAPTER 4 MONITORING OF COMPUTERIZED SYSTEM OPERATIONS

A. INPUT/OUTPUT DEVICE OPERATION.

The accuracy and performance of these devices are vital to the proper operation of the computer system. Improper inputs from thermocouples, RTDs, pressure gauges, etc., can compromise the most sophisticated microprocessor controlled system. These sensors should be systematically calibrated and checked for accurate signal outputs.

Input to and output from the computer system should be checked by the processing firm for accuracy. While this does not mean that every bit of input and output needs to be checked, it does mean that checking must be sufficient to provide a high degree of assurance that input and output is accurate. In this regard there needs to be some reasonable judgment as to the extent and frequency of checking based upon a variety of factors such as the complexity of the computer systems. The right kinds of input edits, for example, could mitigate the need for extensive checks.

During the inspection determine the degree and nature of input/output checks and the use of edits and other built-in audits.

Input/output error handling has been a problem in computerized systems. Determine the firm's error handling procedures including documentation, error verification, correction verification, and allowed error overrides.

An illustration of inadequate input/output checks and error handling would be where a firm used a computer to sense and record retort temperatures during the thermal processing of an LACF. Failure of the firm to verify that the computer is providing an accurate reading of the correct temperature by independent observations of the Mercury-in-Glass thermometer during the thermal process would be a lack of adequate input checks. Failure of the firm to respond in some way to differences between the recorded (computer sensed temperature) and the observed temperature would indicate inadequate error handling. Determine the degree to which the firm's personnel monitor computerized operations. Is such monitoring continuous or periodic, what functions are monitored? For example, a firm's computer system may be used to maintain the pH in a mixing kettle, but if the firm does not sufficiently monitor the system they may fail to detect a hardware problem that allows the pH to go out of tolerance. During the inspection, where possible, spot-check computer operations such as:

1. Calculations; compare manual calculations of input data with the automated calculations or ask the firm to enter a given set of input values and compare automated results against known results.
2. Input recording; compare sensor indications with what the computer indicates, for example. As mentioned previously, some signals may be incorrectly converted and built-in software programming edits may alter input data. For example, a thermocouple indicating 80 C may read out on a view screen as 100 C or any other temperature if the signal converter is malfunctioning.
3. Time keeping; where computers are reporting events and controlling a function in real time, spot-check the time accuracy against a separate time piece; accurate time keeping is especially important where time is a determinative or limiting factor in a food manufacturing process such as during pasteurization or sterilization. It should be noted that some computer systems run on a 12-hour clock whereas others run on a 24-hour clock. When a host computer system is used, determine if the host or the process computer controls the time during process function control, record printing etc. Time keeping conflicts can arise when more than one of the computers is responsible for keeping or indicating time.

   The firm should have a requirement for the computer clock to be reset at predetermined intervals to insure that the system is using the correct time of day. This may be important in continuously operating systems and in those systems documenting the production time of day.

4. Automated cleaning in place (CIP); determine the procedure used, how the firm assures adequacy of cleaning, and residue elimination.

B. ALARMS:

A typical computer system will have several built-in alarms to alert personnel to some out-of-limits situations or malfunctions. Determine what functions are linked to alarms. For example, alarms may be linked to power supply devices, feedback signals to confirm execution of commands, and food process conditions such as empty or overflowing tanks. Determine the alarm thresholds for control of critical functions and whether or not such thresholds can be changed by the operator. For example, if the temperature of water in a pasteurization tank is linked to an alarm which sounds when the temperature drops below 95øC, can the operator change the threshold to 93øC?

Determine how the firm responds when an alarm is activated. This should be covered in the firm's written operating procedures. Determine the types of alarms (lights, buzzers, whistles, etc.) and how the firm assures their proper performance. Are they tested periodically and equipped with in-line monitoring lights to show they are ready? Because an activated alarm may signal a significant out of control situation it is important that such alarm activations are documented. Determine how alarms are documented in production records, in separate logs or automatic electronic recording, for instance. Can all alarm conditions be displayed simultaneously or must they be displayed and responded to consecutively? If an employee is monitoring a CRT display covering one phase of the operation, will that display alert the employee to an alarm condition at a different phase? If so, how? The operation of the computerized systems alarms should be validated as part of the complete computerized system under actual operating conditions.

C. MANUAL BACK-UP SYSTEMS:

Functions controlled by computerized systems may sometimes also be controlled by parallel manual backup systems. During the inspection find out what functions can be manually controlled and identify manual backup devices. Critical process controls are particularly important. Determine the interaction of manual and computerized controls and the degree to which manual intervention can override or defeat the computerized function. The firm's operating instructions should describe what manual overrides are allowed, who may execute them, how and under what circumstances.

Determine if and how manual interventions are documented; a separate log may be kept of such interventions. The computerized system may be such that it detects, reacts to and automatically records manual interventions and this should be addressed during the inspection. It is important that system operators are trained in manual backup systems. Determine the extent of the operator training and if the firm has any procedures for testing the manual backup system on a routine basis (e.g., computer controlled systems would be manually operated for several hours once every month).

D. SHUTDOWN RECOVERY:

How a computer controlled function is handled in the event of computer shutdown (e.g., power failure) is significant and can pose a problem. Shutdown recovery procedures are not uniform in the industry. Some systems, for example, must be restarted from the initial step in the software routine sequence and memory of what has occurred is lost. Other systems have safeguards whereby memory is retained and the control function is resumed at the point where it was halted. Newer systems may have limited battery back-up which will allow the firm to complete the control and/or documentation function or to step the manufacturing process through a safe shutdown procedure. Determine the disposition of the computer's memory content (program and data) upon computer shutdown.

Determine the firm's shutdown recovery procedure and if, in the event of computer failure, the food manufacturing process or control function is brought into a "safe" condition to protect the product. Determine such safeguards and how they are implemented. Where is the point of restart in the cycle - at the initial step, a random step or the point of shutdown? Look for the inappropriate duplication of steps in the resumption of the process. The time it takes to resume a computerized process or switch to manual processing can be critical, especially where failure to maintain process conditions for a set time (e.g. temperature control during the thermal processing of LACF) compromises product integrity. Therefore, note recovery time for delay-sensitive functions and investigate instances where excessive delays compromise product safety or where established time limits are exceeded. Many systems have the ability to be run manually in the event of computer shutdown. It is important that such backup manual systems provide adequate function control and documentation. Determine if backup manual controls (valves, gates, etc.) are sufficient to control the food manufacturing process and if employees are familiar with their operation. Records of manual operations may be less detailed, incomplete, and prone to error, compared to computerized documentation, especially when they are seldom exercised. Therefore, determine how manual operations are documented and if the information recorded manually conforms with CGMP requirements.

The computerized systems shutdown and recovery process should be validated as part of the validation of the computerized system under actual operating conditions.

REFERENCES:

Software Development Activities Report, Feb. 1987, U.S. Food and Drug Administration, Office of Regulatory Affairs.

Guide to Inspection of Computerized Systems in Drug Processing, Feb. 1983, U.S. Food and Drug Administration, Office of Regulatory Affairs.

Guideline on General Principles of Process Validation, May 1987, U.S. Food and Drug Administration, Office of Regulatory Affairs.

Glossary of Computerized System and Software Development Terminology, August 1995, U.S. Food and Drug Administration, Office of Regulatory Affairs.

Guide to Inspection of LACF Manufacturers - Part 1 - Administrative Procedures/Scheduled Processes, November 1996; Part 2 - Processes/Procedures, April 1997; and Part 3 - (currently in draft, not yet released), U.S. Food and Drug Administration, Office of Regulatory Affairs.

Guide to Inspections of Dairy Product Manufacturers, April 1995, U.S. Food and Drug Administration, Office of Regulatory Affairs.

Guide to Inspections of Miscellaneous Food Products - Volume 1, May 1995, U.S. Food and Drug Administration, Office of Regulatory Affairs.

Guide to Inspections of Miscellaneous Food Products - Volume 2, October 1996, U.S. Food and Drug Administration, Office of Regulatory Affairs.

Guide to Inspections of Interstate Carriers and Support Facilities, April 1995, U.S. Food and Drug Administration, Office of Regulatory Affairs.

Inspectional Methods (Interim Guidance), October 1996, U.S. Food and Drug Administration, Office of Regulatory Affairs.

FDA Final Rule on Electronic Signatures, 21 CFR Part 11, published March 20, 1997.

Current Good Manufacturing Practice, Quality Control Procedures, Quality Factors, Notification Requirements, and Records and Reports, for the Production of Infant Formula; Proposed Rule, Federal Register July 09, 1996.

APPENDIX 1 - QUICK GUIDE TO EVALUATION OF COMPUTERIZED SYSTEMS USED IN FOOD PROCESSING

This appendix is provided as a quick reference guide for use by FDA investigators conducting inspections of food manufacturing plants using computer control/documentation systems. The guide should not be used without a through understanding of the information provided in the main text of the Guide To Inspection of Computerized Systems in the Food Processing Industry.

1.) Determine the critical control points in the food process using HACCP concepts. Examples would be:

Pasteurization

Sterilization

pH control

Nutrient control/weighing

Nutrient analysis

Record keeping

Control of microbiological growth

2.) For those critical control points controlled by computerized systems determine if failure of the computerized system may cause food adulteration. Is the critical control point covered by GMP's or the FD&C Act?

3.) Identify computerized system components including:

Hardware:

Input devices

Output devices

Signal converters

Central Processing Unit

Distribution system

Peripheral devices

Alarms:

Types (visual, audible etc)

Functions

Records

Software:

Documentation:

Manuals

Operating procedures

Personnel:

Type

Training

4.) For computer hardware determine the manufacturer, make and model number.

5.) Obtain or make a simplified drawing of the computerized system control loop including:

Sensors

CPU

Signal converters

Actuators

Peripheral devices

6.) Software:

a. For all critical software determine:

Name

Function

Inputs

Outputs

Set-points

Edits

Input Manipulation of Data

Program Over-rides

b. Who developed software.

c. Software security to prevent unauthorized changes.

d. Firms checks on computerized systems inputs/outputs.

7.) Observe the system as it operates to determine if:

Critical processing limits are met

Records are accurate

Sensor input is accurate

Time keeping is accurate

Personnel are trained in systems operations and functions

8.) Determine if the operator or management can override computer functions. Explain.

9.) Explain how the system handles deviations from set or expected results.

10.) Determine the validation steps used to insure that the computerized system is functioning as designed.

a. Was the computerized system validated upon installation?

Under worst case conditions?

Minimum of 3 test runs?

b. Are there procedures for routine maintenance and revalidation?

Does the equipment in-place meet the original specifications?

c. Is validation of the computerized system documented?

d. How often is system:

maintenance performed

revalidated

calibrated

11.) Are system components located in a hostile environment which may effect their operation?

12.) Determine if the computerized system can be operated manually. Explain.

13.) Automated CIP (cleaning in place).

How does firm ensure that cleaning is adequate.

Documentation of CIP steps.

14.) Shutdown Procedures

Does firm use battery backup system?

Is computer program retained in control system?

What is firms procedure in event power is lost to computer control system?

15.) Does the firm have a documented system for making changes to the computerized system which explains:

The reason for the change

The date of the change

The changes made to the system

Who made the changes

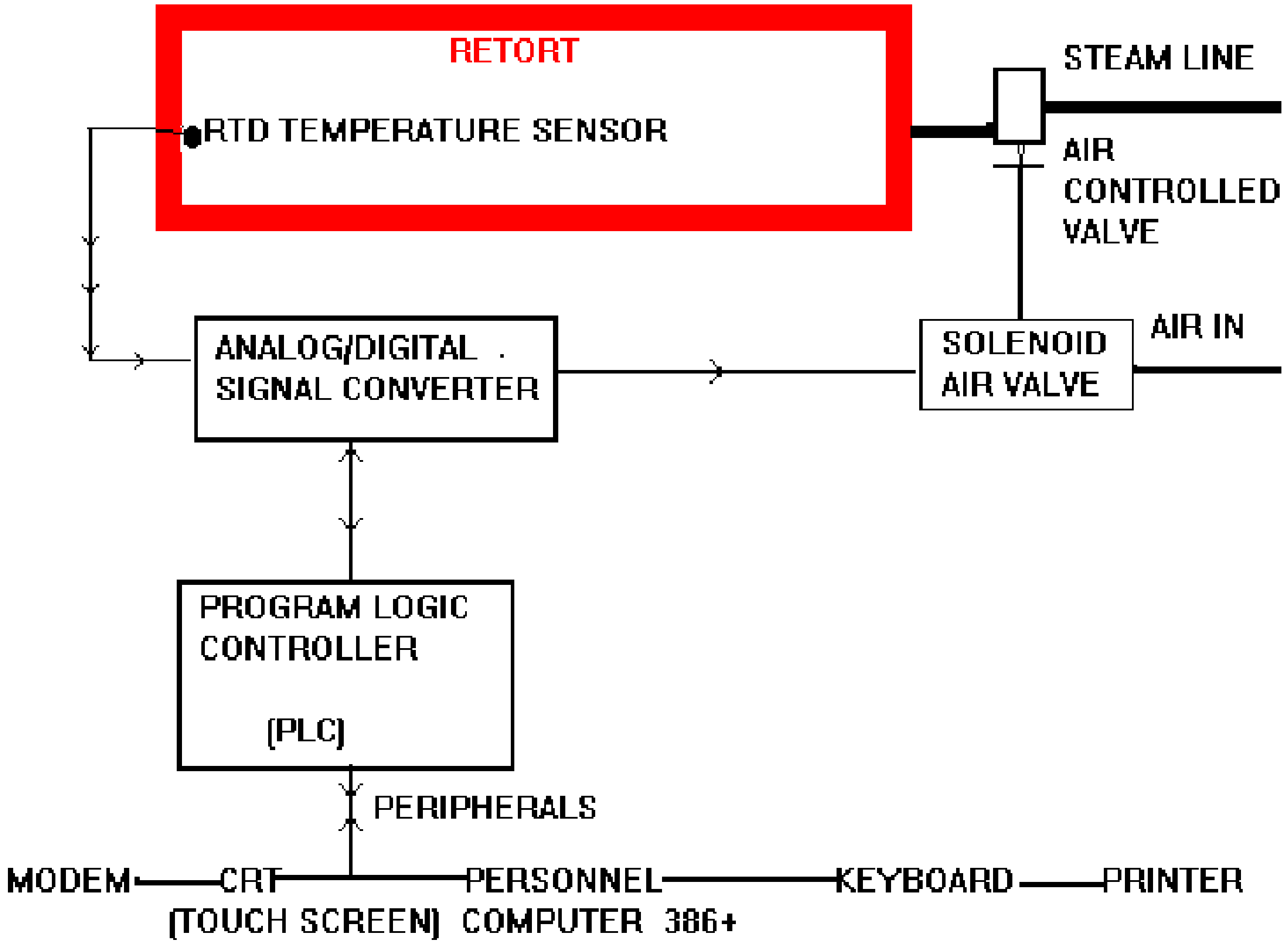
16.) Document computer functions which are causing or may cause food products to be adulterated or misbranded.

APPENDIX 2 **DIAGRAM OF LOGIC CIRCUIT**

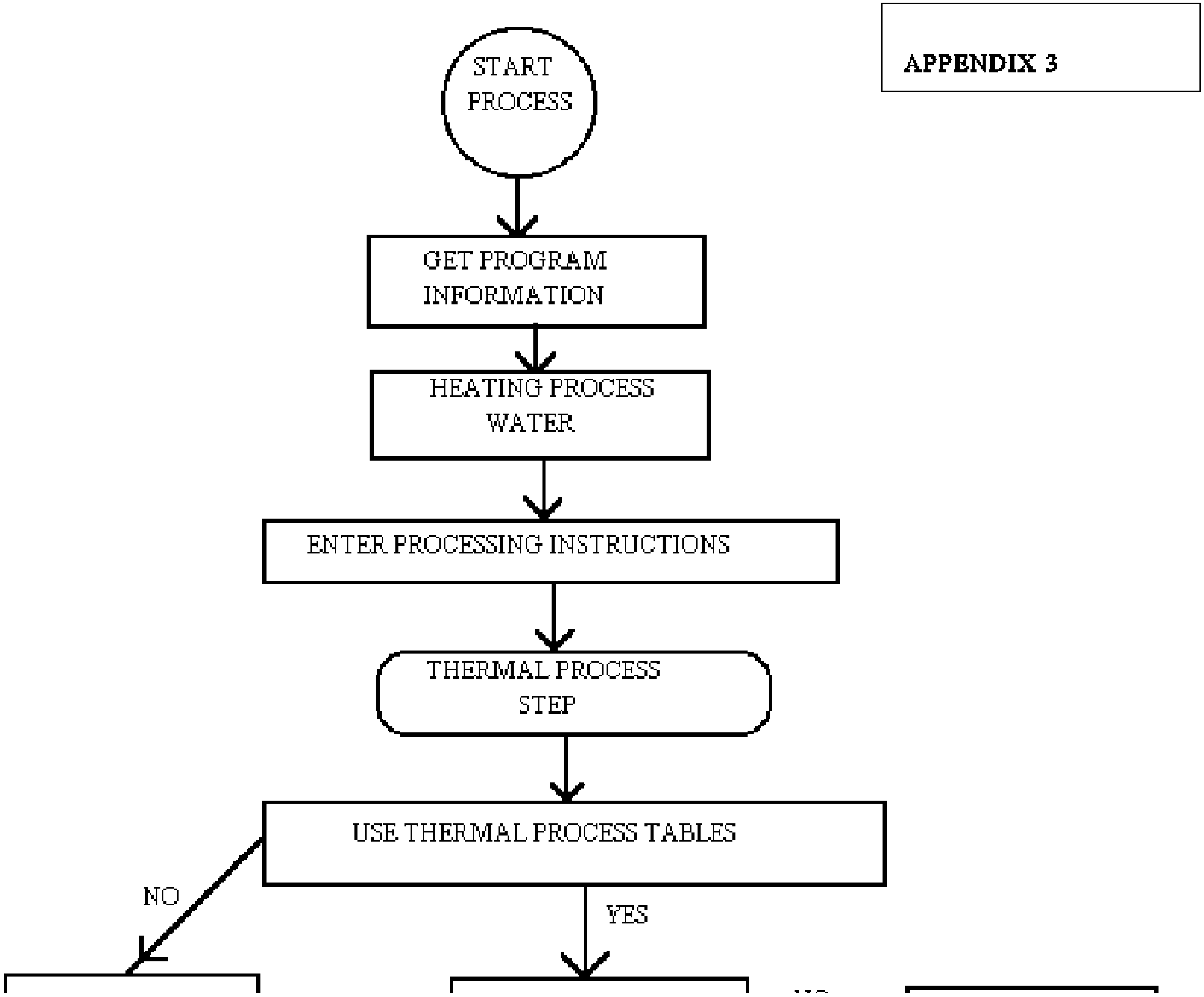
APPENDIX 3 **DIAGRAM OF ALGORITHM**

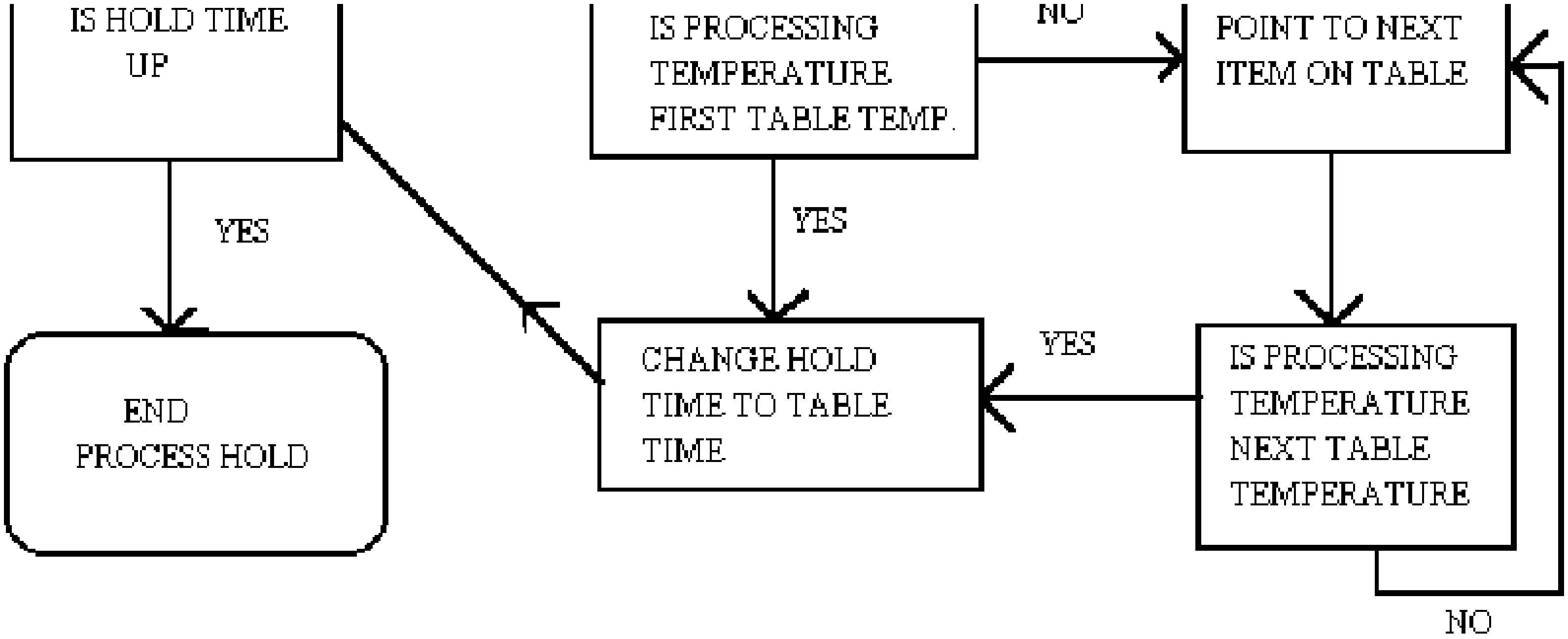
REPRESENTATIVE DIAGRAM OF A PORTION OF AN ALGORITHM FOR A WATER IMMERSION RETORT WHICH CONTROLS THE PROCESS TIME AND TEMPERATURE

RETORT SYSTEM COMPUTER CONTROLLED



APPENDIX 3


START PROCESS
GET PROGRAM INFORMATION
HEATING PROCESS WATER
ENTER PROCESSING INSTRUCTIONS
THERMAL PROCESS STEP
USE THERMAL PROCESS TABLES
NO
YES


IS HOLD TIME
UP
IS PROCESSING
TEMPERATURE
FIRST TABLE TEMP.
NO
POINT TO NEXT
ITEM ON TABLE
YES
YES
CHANGE HOLD
TIME TO TABLE
TIME
YES
IS PROCESSING
TEMPERATURE
NEXT TABLE
TEMPERATURE
END
PROCESS HOLD
NO